EUROPEAN PATENT APPLICATION

(54) **Public key/signature cryptosystem with enhanced digital signature certification.**

(57) A public key cryptographic system is disclosed with enhanced digital signature certification which authenticates the identity of the public key holder. A hierarchy of nested certifications and signatures are employed which indicate the authority and responsibility levels of the individual whose signature is being certified. The present invention enhances the capabilities of public key cryptography so that it may be employed in a wider variety of business transactions, even those where two parties may be virtually unknown to each other. Counter-signature and joint-signature requirements are referenced in each digital certification to permit business transactions to take place electronically, which heretofore often only would take place after at least one party physically winds his way through a corporate bureaucracy. The certifier in constructing a certificate generates a special message that includes fields identifying the public key which is being certified, and the name of the certifiee. In addition, the certificate constructed by the certifier includes the authority which is being granted including information which reflects issues of concern to the certifier such as, for example, the monetary limit for the certifiee and the level of trust which is granted to the certifiee. The certificate may also specify cosignature requirements which are being imposed upon the certifiee.

FIG.2 CREATE SIGNATURE

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl.4)
X	C.POMERANCE: "ADVANCES IN CRYPTOLOGY-CRYPTO '87" 1987, SPRINGER VERLAG, BERLIN * page 212, line 2 - page 214, line 3 * ---	1, 2, 10, 11	H04L9/00
A	COMPUTERS & SECURITY. vol. 6, no. 3, June 1987, AMSTERDAM NL pages 206 - 218; K.RIHACZEK: "TELETRUST-OSIS AND COMMUNICATION SECURITY" * page 210, right-hand column, line 10 - page 211, left-hand column, line 19 * * right-hand column, lines 13 - 32 * ------	1, 4, 5, 13	

			TECHNICAL FIELDS SEARCHED (Int. Cl.4)
			H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	15 OCTOBER 1990	HOLPER G.E.E.

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another
    document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or
    after the filing date
D : document cited in the application
L : document cited for other reasons

....
& : member of the same patent family, corresponding
    document

(12) **EUROPEAN PATENT APPLICATION**

(71) Applicant: Fischer, Addison M.
60 14th Avenue South
Naples Florida 33940(US)

(72) Inventor: Fischer, Addison M.
60 14th Avenue South
Naples Florida 33940(US)

(74) Representative: Evershed, Michael et al
Saunders & Dolleymore 9, Rickmansworth
Road
Watford Hertfordshire WD1 7HE(GB)

(54) Public key/signature cryptosystem with enhanced digital signature certification.

(57) A public key cryptographic system is disclosed with enhanced digital signature certification which authenticates the identity of the public key holder. A hierarchy of nested certifications and signatures are employed which indicate the authority and responsibility levels of the individual whose signature is being certified. The present invention enhances the capabilities of public key cryptography so that it may be employed in a wider variety of business transactions, even those where two parties may be virtually unknown to each other. Counter-signature and joint-signature requirements are referenced in each digital certification to permit business transactions to take place electronically, which heretofore often only would take place after at least one party physically winds his way through a corporate bureaucracy. The certifier in constructing a certificate generates a special message that includes fields identifying the public key which is being certified, and the name of the certifiee. In addition, the certificate constructed by the certifier includes the authority which is being granted including information which reflects issues of concern to the certifier such as, for example, the monetary limit for the certifiee and the level of trust which is granted to the certifiee. The certificate may also specify cosignature requirements which are being imposed upon the certifiee.

EP 0 328 232 A2

PUBLIC KEY/SIGNATURE CRYPTOSYSTEM WITH ENHANCED DIGITAL SIGNATURE CERTIFICATION

FIELD OF THE INVENTION

This invention relates to a cryptographic communications system and method. More particularly, the
5 invention relates to a public key or signature cryptosystem having improved digital signature certification for
indicating the identity, authority and responsibility levels associated with at least the sender of a digital
message.

BACKGROUND AND SUMMARY OF THE INVENTION
10

The rapid growth of electronic mail systems, electronic funds transfer systems and the like has
increased concerns over the security of the data transferred over unsecured communication channels.
15 Cryptographic systems are widely used to insure the privacy and authenticity of messages communicated
over such insecure channels.

In a conventional cryptographic system, a method of encryption is utilized to transform a plain text
message into a message which is unintelligible. Thereafter, a method of decryption is utilized for decoding
the encrypted message to restore the message to its original form.
20 Conventional crypotographic signature and authentication systems typically utilize a "one way" hashing
function to transform the plain text message into a form which is unintelligible. A "hashing" function as used
herein is a function which can be applied to an aggregation of data to create a smaller, more easily
processed aggregation of data.

An important characteristic of the hashing function is that it be a "one-way" function. A hash is a "one-
25 way" function, if it is far more difficult to compute the inverse of the hashing function than it is to compute
the function. For all practical purposes, the value obtained from applying the hashing function to the original
aggregation of data is an unforgeable unique fingerprint of the original data. If the original data is changed
in any manner, the hash of such modified data will likewise be different.

In conventional cryptographic systems, binary coded information is encrypted into an unintelligible form
30 called cipher and decrypted back into its original form utilizing an algorithm which sequences through
encipher and decipher operations utilizing a binary code called a key. For example, the National Bureau of
Standards in 1977 approved a block cipher algorithm referred as the Data Encryption Standard (DES). Data
Encryption Standard, FIPS PUB 46, National Bureau of Standards, January 15, 1977.

In DES, binary coded data is cryptographically protected using the DES algorithm in conjunction with a
35 key. Each member of a group of authorized users of encrypted computer data must have the key that was
used to encipher the data in order to use it. This key held by each member in common is used to decipher
the data received in cipher form from other members of the group.

The key chosen for use in a particular application makes the results of encrypting data using the DES
algorithm unique. Selection of a different key causes the cipher that is produced for a given set of inputs to
40 be different. Unauthorized recipients of the cipher text who know the DES algorithm, but who do not have
the secret key, cannot derive the original data algorithmically.

Thus, the cryptographic security of the data depends on the security provided for the key used to
encipher and decipher the data. As in most conventional cryptographic systems the ultimate security of the
DES system critically depends on maintaining the secrecy of the cryptographic key. Keys defined by the
45 DES system include sixty-four binary digits of which fifty-six are used directly by the DES algorithm as the
significant digits of the key and eight bits are used for error detection.

In such conventional cryptographic systems, some secure method must be utilized to distribute a secret
key to the message sender and receiver. Thus, one of the major difficulties with existing cryptographic
systems is the need for the sender and receiver to exchange a single key in such a manner that an
50 unauthorized party does not have access to the key.

The exchange of such a key is frequently done by sending the key, prior to a message exchange, via,
for example, a private courier or registered mail. While providing the necessary security such key
distribution techniques are usually slow and expensive. If the need for the sender and receiver is only to
have one private message exchange, such an exchange could be accomplished by private courier or
registered mail, thereby rendering the cryptographic communication unnecessary. Moreover, if the need to

communicate privately is urgent the time required to distribute the private key causes an unacceptable delay.

Public key cryptographic systems solve many of the key distribution problems associated with conventional cryptographic systems. In public key cryptographic systems the encrypting and decrypting processes are decoupled in such a manner that the encrypting process key is separate and distinct from the decrypting process key. Thus, for each encryption key there is a corresponding decryption key which is not the same as the encryption key. Even with knowledge of the encryption key, it is not feasible to compute the decryption key.

With a public key system, it is possible to communicate privately without transmitting any secret keys. The public key system does require that an encryption/decryption key pair be generated. The encryption keys for all users may be distributed or published and anyone desiring to communicate simply encrypts his or her message under the destination user's public key.

Only the destination user, who retains the secret decrypting key, is able to decipher the transmitted message. Revealing the encryption key discloses nothing useful about the decrypting key, i.e., only persons having knowledge of the decrypting can decrypt the message. The RSA cryptographic system which is disclosed in U.S. Patent No. 4,405,829 issued to Rivest et al discloses an exemplary methodology for a practical implementation of a public key cryptographic system.

A major problem in public key and other cryptographic systems is the need to confirm that the sender of a received message is actually the person named in the message. An authenticating technique known utilizing "digital signatures" allows a user to employ his secret key to "sign a message" which the receiving party or a third party can validate using the originator's public key. See for example U.S. Patent No. 4,405,829.

A user who has filed a public key in a publicly accessible file can digitally sign a message by decrypting the message or a hash of it with the user's private key before transmitting the message. Recipients of the message can verify the message or signature by encrypting it with the sender's public encryption key. Thus, the digital signature process is essentially the reverse of the typical cryptographic process in that the message is first decrypted and then encrypted. Anyone who has the user's public encryption key can read the message or signature, but only the sender having the secret decryption could have created the message or signature.

Serious problems still persist in public key cryptosystems of assuring that a specified public key is that actually created by the specified individual. One known technique for addressing this problem is to rely on some trusted authority, e.g., a governmental agency, to insure that each public key is associated with the person who claiming to be the true author.

The trusted authority creates a digital message which contains the claimant's public key and the name of the claimant (which is accurate to the authority's satisfaction) and a representative of the authority signs the digital message with the authority's own digital signature. This digital message, often known as a certificate, is sent along with the user of the claimant's own digital signature. Any recipient of the claimant's message can trust the signature, provided that the recipient recognizes the authority's public key (which enables verification of the authority's signature) and to the extent that the recipient trusts the authority.

Prior to the present invention, the transmitted certificate failed to provide any indication of the degree of trust or the level of responsibility with which the sender of the message should be empowered. Instead, the certification merely indicates that the identified trusted authority recognized the sender's public key as belonging to that person.

The public key system is designed to operate such that the public keys of various users are published to make private communications easier to accomplish. However, as the number of parties who desire to use the public key system expands, the number of published keys will soon grow to a size where the issuing authority of the public keys can not reasonably insure that the parties whose public keys are published are, in fact, the people who they are claiming to be. Thus, a party may provide a public key to be maintained in the public directory under the name of the chairman of a major corporation, e.g., for example, General Motors Corporation. Such an individual may then be in a position to receive private messages directed to the chairman of General Motors or to create signatures which ostensibly belong to the impersonated chairman.

There are also technologies for producing digital signatures which may not require full public key capability, including, for example, the Fiat-Shamir algorithm. Any digital signature methodology may be employed to implement the digital signatures referenced herein. Any reference to public key cryptosystems should also be construed to reflect signature systems. Any reference to public key decryption should be taken as a generalized reference to signature creation and any reference to encryption should be taken as a reference to signature verification.

3

The present invention addresses such problems with the public key or signature cryptographic system relating to authenticating the identity of the public key holder by expanding the capability of digital signature certification. In this regard, a certification methodology is utilized which employs multiple level certification while at the same time indicating the authority and responsibility levels of the individual whose signature is being certified as is explained in detail below.

The present invention enhances the capabilities of public key cryptography so that it may be employed in a wider variety of business transactions, even those where two parties may be virtually unknown to each other.

The digital signature certification method and apparatus of the present invention provides for a hierarchy of certifications and signatures. It also allows for co-signature requirements. In this regard, counter-signature and joint-signature requirements are referenced in each digital certification to permit business transactions to take place electronically, which heretofore often only would take place after at least one party physically winds his way through a corporate bureaucracy.

In the present invention, a digital signature is certified in a way which indicates the authority the has been granted to the party being certified the certifiee). The certifier in constructing a certificate generates a specialmessage that includes fields identifying the public key which is being certified, and the name of the certifiee. In addition, the certificate constructed by the certifier includes the authority which is being granted and limitations and safeguards which are imposed including information which reflects issues of concern to the certifier such as, for example, the monetary limit for the certifiee and the level of trust which is granted to the certifiee. The certificate may also specifyco-signature requirements as being imposed upon the certifiee

The present invention further provides for certifying digital signatures such that requirement for further joint certifying signatures is made apparent to any receiver of a digital message. The requirement for joint signatures is especially useful in transactions where money is to be transferred or authorized to be released. To accomplish this end, the certificate of the present invention is constructed to reflect (in addition to the public key and the name of the certifiee and other fields) the number of joint signatures required and an indication as to the identity of qualifying joint signers. Thus, an explicit list of each of the other public key holders that are required to sign jointly may be included in the. certificate. In this fashion, the recipient is informed that any material which is signed by the authorityof the sender's certificate, must also be signed by a number of other specified signators. The recipient is therefore able to verify other joint and counter signatures by simply comparing the public keys present in each signature in the certificate. The present invention also includes other ways of indicating co-signature requirements such as by indicating other certificates. Such indications of other public key holders may be explicit (with a list as described here), or implicitly, by specifying some other attribute or affiliation. This attribute or affiliation may also be indicated in each co-signer' certificate.

Additionally, the present invention provides for the certification of digital signatures such that a trust level is granted to the recipient for doing subcertifications. In this manner, a trust level of responsibility flows from a central trusted source.

In an exemplary embodiment of the present invention, a certifier is permitted to assign with one predetermined digital code a trust level which indicates that the certifier warrants that the user named in the certificate is known to the certifier and is certified to use the associated public key. However, by virtue of this digital code, the user is not authorized to make any further identifications or certifications on the certifier's behalf. Alternatively, the certifier may issue a certificate having other digital codes including a code which indicates that the user of the public key is trusted to accurately identify other persons on the certifier's behalf and is further trusted to delegate this authority as the user sees fit.

The present invention further provides for a user's public key to be certified in multiple ways (e.g., certificates by different certifiers). The present invention contemplates including the appropriate certificates as part of a user's signed message. Such certificates include a certificate for the signer's certifier and for the certifiers' certifier, etc., up to a predetermined certificate which is trusted by all parties involved. When this is done, each signed message unequivocally contains the ladder or hierarchy of certificates and the signatures indicating the sender's authority. A recipient of such a signed message can verify that authority such that business transactions can be immediately made based upon an analysis of the signed message together with the full hierarchy of certificates.

BRIEF DESCRIPTION OF THE DRAWINGS

These as well as other features of this invention will be better appreciated by reading the following description of the preferred embodiment of the present invention taken in conjunction with the accompanying drawings of which

FIGURE 1 is a exemplary block diagram of a cryptographic communications system in accordance
5 with an exemplary embodiment of the present invention;

FIGURE 2 is a flow diagram that indicates how a digital signature is created in accordance with an exemplary embodiment of the present invention;

FIGURE 3 is a flow diagram that indicates how a digital signature created in accordance with FIGURE 2 is verified;

10 FIGURE 4 is a flow diagram that indicates how a countersignature is created for a digital signature;

FIGURE 5 is a flow diagram that indicates how a digital certificate in created in accordance with an exemplary embodiment of the present invention;

FIGURE 6 is a flow diagram that indicates how a joint signature is added to a certificate; and

FIGURE 7 is a flow diagram that indicates how the signatures and certificates are verified by a
15 recipient of the transmitted message.

DETAILED DESCRIPTION OF THE PRESENTLY PREFERRED EMBODIMENT

20

Figure 1 shows in block diagram form an exemplary communications system which may be used in conjunction with the present invention. This system includes an unsecured communication channel 12 over which communications between terminals A,B ... N may take place. Communication channel 12 may, for
25 example, be a telephone line. Terminals A,B through N may, by way of example only, be IBM PC's having a processor (with main memory) 2 which is coupled to a conventional keyboard/CRT 4. Each terminal A,B through N also includes a conventional IBM PC communications board (not shown) which when coupled to a conventional modem 6, 8, 10, respectively, permits the terminals to transmit and receive messages.

Each terminal is capable of generating a plain text or unenciphered message, transforming the message
30 to an encoded, i.e., enciphered form, and transmitting the message to any of the other terminals connected to communications channel 12 (or to a communications network (not shown) which may be connected to communications channel 12). Additionally, each of the terminals A,B through N is capable of decrypting a received enciphered message to thereby generate a message in plain text form.

Each of the terminal users (as discussed above with respect to public key systems) has a public
35 encrypting key and an associated private secret decrypting key. In the public key cryptosystem shown in Figure 1, each terminal user is aware of the general method by which the other terminal users encrypt a message. Additionally, each terminal user is aware of the encryption key utilized by the terminal's encryption procedure to generate the enciphered message.

Each terminal user, however, by revealing his encryption procedure and encryption key does not reveal
40 his private decryption key which is necessary to decrypt the ciphered message and to create signatures. In this regard, it is simply not feasible to compute the decryption key from knowledge of the encryption key. Each terminal user, with knowledge of another terminal's encryption key, can encrypt a private message for that terminal user. Only the terminal end user with his secret decrypting key can decrypt the transmitted message.

45 Besides the capability of transmitting a private message, each terminal user likewise has the capability of digitally signing a transmitted message. A message may be digitally signed by a terminal user decrypting a message with his private decrypting key before transmitting the message. Upon receiving the message, the recipient can read the message by using the sender's public encryption key. In this fashion, the recipient can verify that only the holder of the secret decryption key could have created the message.
50 Thus, the recipient of the signed message has proof that the message originated from the sender. Further details of a digital signature methodology which may be used in conjunction with the present invention is disclosed in U.S. Patent No. 4,405,829.

Before describing the details of the enhanced digital certification in accordance with the present invention, the general operation of Figure 1 in an electronic mail, public key cryptographic context will
55 initially be described. Initially, presume that the user of terminal A is a relatively low level supervisor of a General Motors computer automated design team who wishes to purchase a software package from a computer software distributor located in a different state. The computer software distributor has terminal N and an associated modem 10 located at his store.

5

The General Motors supervisor at terminal A constructs an electronic purchase order which identifies the item(s) being ordered and the address to which the items must be sent as well as other items which are necessary in a standard purchase order. It should be recognized that, although this example relates to an electronic purchase order, any aggregation of data which can be represented in a manner suitable for

5 processing with whatever public-key method is being used for signatures may likewise be transmitted. In the more detailed description which follows such an aggregation of data, e.g., a computer data file, will generically be referred to as an "object".

The terminal A user, the General Motors supervisor, digitally signs the purchase order under the authority of a certificate which is appended to the transmitted message which will be discussed further

10 below. Turning first to the supervisor's digital signature, a message can be "signed" by applying to at least a portion of the object being signed, the privately held signature key. By signing an image of the object (or a more compact version thereof known as a digest or hash of the object to be explained in more detail below) with the secret key, it is possible for anyone with access to the public key to encrypt this result and compare it with the object (or a recomputed hash or digit version thereof). Because only the owner of the

15 public key could have used the secret key to perform this operation, the owner of the public key is thereby confirmed to have signed the message.

In accordance with the present invention, a digital signature is additionally accompanied by at least one valid certificate which specifies the identity of the signer and the authorization which the signer has been granted. The certificate may be viewed as a special object or message which specifies the identity of the

20 user of a particular public key and the authority which has been granted to that user by a party having a higher level of authority than the user.

To be valid a certificate must be signed by the private key(s) associated with one or more other valid certificates which are hereafter referred to as antecedents to that certificate. Each of these antecedent certificates must grant the signer the authority to create such a signature and/or to issue the purchase order

25 in our example. Each of the antecedent certificates may in turn have its own antecedent(s).

An exemplary embodiment of the present invention contemplates utilizing an ultimate antecedent certificate of all certificates, which is a universally known and trusted authority, e.g., hypothetically the National Bureau of Standards, and which is referred to as a meta-certificate. The meta certificate is the onlyitem that needs to be universally trusted and known. There may be several meta-certifiers, and it is

30 possible that meta-certificates may even reference each other for required co-signatures.

Turning back to our example, when the message is ultimately transmitted from terminal A to the computer software distributor at terminal N, the recipient in a manner which will be described in detail below, verifies the signature of the General Motors supervisor. Additionally, he verifies that all the other signatures on the message certificate and the antecedent certificates are present which provides further

35 assurance to the terminal N software distributor that the transaction is a valid and completely authorized. As should be recognized, such assurances are critically important prior to shipping purchased items and are perhaps even more important in an electronic funds transfer context.

Any party who receives a message transmitted by the user of terminal A (whether such a party is the ultimate recipient of the message at terminal N or other parties within for example a corporate hierarchy

40 such as General Motors) can verify and validate A's signature and the authority that the terminal A user exercised. Such validation is possible since a complete hierarchy of validating certificates is transmitted with the original purchase order which permits the ultimate recipient to feel confident that the requested transaction is authentic and properly authorized.

Focussing more generically on major transactions emanating from, for example, General Motors

45 Corporation, it is helpful to focus first on the ultimate certifier(s) mentioned above, i.e., the meta-certifiers. In this regard, General Motors and parties who plan to do business with General Motors or otherwise participate in the public key cryptosystem may initially choose to approach a universally recognized trusted authority e.g., hypothetically the Bureau of Standards and/or one of the country's largest banks. Corporate and other participants in this system register a set of public keys (which they are authorized to use by

50 virtue of an action of their corporate board of directors) with the meta-certifier. These are "high level" keys to be used within the General Motors environment primarily for certifying General Motors' internal personnel. The meta-certifier in return distributes to General Motors its certification that each of these supplied public keys created by General Motors is authorized for their own use. In effect, the meta-certifier is certifying that the party using each key is actually associated with General Motors. The meta-certifier's

55 certification may include embedded text which indicates that the users of registered public keys are properly associated with General Motors. For example, General Motors may decide to have three "high level" keys certified, e.g., corporate officers, such as the vice president, financial officer, and the security officer. At General Motors' request each of the three certificates indicate the public keys of the other two as

6

required joint signatures.

Thus, once having obtained the highest level certificate(s) from the meta-certifier, several officials within General Motors may have to jointly sign certificates at the next lower level and such joint signatures. Each of these high level General Motors' certificates would mutually reference each other as required co-signers A this level no single corporate officer acting alone may authorize anything because embedded within each of the three certificates is a requirement for the signature of others who are specifically identified. In turn then, these 3 officers create and sign public keys for the other General Motors' employees, that define exactly the level of authority, responsibility and limitations each employee is to have. One of these certificates may belong to user A, or will be an antecedent to user's A's certificate.

Each of these three high level certificates may digitally sign terminal B user's certificate preferably after a face to face or telephone verification. After each of the required signatures has been created, the certificate's signatures by the vice president, financial officer and security officer as well as their respective 3 certificates, as well as those certificates' respective signatures by the meta-certifier are ultimately returned to the General Motors' supervisor at terminal B to be stored for ongoing use, such as in our example for subcertifying terminal user A. In this manner, the signed message unequivocally contains the ladder or hierarchy of certificates and signatures verifying terminal A user's identify and his authority.

When a party B in a ladder of certifications creates an authorizing certificate for party A, the certificate includes a specification of A's identity together with A's public encryption key. Additionally, the certificate indicates the authority, capabilities and limitations which B wishes to grant A. By granting this certificate B explicitly assumes responsibility for both A's identity and authority.

B's certificate for A also permits a specification of other parties who are required to cosign actions taken by A when using this certificate as will be explained further below. Cosignatures may take the form of either joint signatures or countersignatures. Additionally party B can define in the certificate for A the degree to which B will recognize subcertifications performed by A.

In accordance with an exemplary embodiment of the present invention, trust levels which are granted by the certifier to the certifiee are specified in the certificate by a predetermined digital code. Such a trust level is used by the recipient of the message as an indicator of the authority granted to the certifiee and the responsibility assumed by the certifier for the certifiee's actions with respect to the use of the public key being certified.

By way of example only trust levels may be indicated by trust level values 0, 1, 2, and 3.

Trust level 0 indicates that the certifier vouches that the certified public key belongs to the individual named in the certificate; but that the certifier will not assume responsibility for the accuracy of any certificates produced by the certifiee. The essence of this would be a statement by the certifier that: "I warrant the user named in this certificate is known to me and is being certified to use the associated public key --however I do not trust him to make any further indentifications on my behalf".

Trust level 1 empowers the certifiee to make level 0 certifications on behalf of the certifier. The essence of this would be a statement by the certifier that: "I know the user of this public key and I trust him/her to accurately identify other persons on my behalf. I will take responsibility for such identifications. However, I do not trust this person to identify persons as trustworthy." Trust level 2 empowers the certifiee to make level 0, 1 and 2 certifications on behalf of the certifier. The essence of this would be a statement by the certifier that : "I know the user of this public key and I trust him/her to accurately identify other persons on my behalf, and I furthermore trust them to delegate this authority as they see fit. I assume due responsibility for any certifications done by them or any duly authorized agent created by them or by other generation of duly created agents".

Trust level 3 is reserved exclusively for an ultimate meta certifier whose public key and certificate is established and also well known (possibly by repetitive and widespread media publication) and whose accuracy is universally respected. This certifier takes responsibility only for accurately identifying the entities whose public keys it certifies. It assumes no responsibility for the use of these keys.

Additionally, each certification may specify the monetary limit, i.e., the maximum amount of money value which the certifiee is authorized to deal with. The monetary limit must not of course exceed the limit in the certifier's own certificate to insure that the certifier does not delegate more than he is allowed to handle.

Before discussing further details of the digital signature and certification techniques of the present invention, it may be helpful to first define certain terminology. As noted above, the term "object" is generically used to describe any aggregation of data that can be ultimately represented in a manner suitable for processing with whatever public key method is being utilized for signatures and/or encryption. The term object may apply to a "primary" object such as a purchase order or check, or money transfer; or to a "secondary" object such as a certificate, or another signature.

7

The methodology of the present invention in order to increase processing efficiency generally applies a function to the object to create a generally smaller, more compact, more easily processed object, i.e., typically a fixed size bit string of several dozen or more bits. Such a function is referred to as a hash or digest of the object.

5 An example of such a hash or digest would be the output obtained by processing an image of the object with the data encryption standard (DES) using cipher block chaining mode (CBC). Processing may be done with two different DES keys (both of which are fixed, non-secret and commonly known). Thereafter, each of the final output chaining values are concatenated or merged in some way to become the several dozen or more bits constituting the digest or hash value.

10 An important characteristic of the digest or hashing algorithm is that, while it is easy to compute the digest of an object it is essentially impossible to construct a different or modified object with an equal digest. For all practical purposes the digest is an unforgeable unique fingerprint of the original object. If the original object is changed in any manner, the digest will be different. In other words, for all practical purposes, the more compact representation of the original object is unique to the original object. Ideally, 15 also a hash should not reveal any clue about specific data values contained within the message. The hash's contemplated in the exemplary embodiment have at least 128 bits.

Turning now to Figure 2, this figure shows the data flow and the manner in which signatures are created. The signature process applies not only to general objects such as arbitrary computer files, letters, electronic purchase orders, etc., but also to specialized objects such as signatures and certificates.

20 Each digital signature is accompanied, as is generally shown in Figure 2, by a certification of the public key performing the signature. The certificate, as will be discussed in detail in conjunction with Figure 5, is signed by one or more higher authorities (i.e., the immediate certifiers) and identifies the original signer while specifying the degree of authority which has been granted to the original signer.

In accordance with the present invention, the original signer may have more than one certificate and 25 may utilize different certificates for different levels of authority. Each of the certificates may carry different limitations and requirements including different money limitations, trust levels, joint signature requirements and counter signature requirements.

It is incumbent on the signer to select the appropriate signature/certificate with which to sign a particular object. For example, purchase orders may require a different type of authority (and therefore a different 30 certificate) than merely a letter of inquiry. Thus, the certificate is a very important portion of the transmitted message in that it identifies the signer as well as the signer's level of authority.

As shown in Figure 2, in creating the signature the user utilizes the object 20 (which may, for example, be a purchase order) and specifies the type of object 22. The documentation added under the type of object field, for example, indicates that the object is a purchase order data file. In other instances the type 35 of object field 22 would identify that the object is another signature or a certificate. As indicated at 24, the date of the signature is also identified.

The comment field 26 is utilized to add documentation which, for example, places limitations on the signature or adds other commentary. The signer may indicate that his signature or the object is only good and valid for a predetermined period of time. Additionally, any desired comments regarding the particular 40 transaction, e.g., the purchase order, may be added as comment data.

Also incorporated in the signature is the original signer's certificate 28 which includes the original signer's public key 30 and numerous other fields which are discussed in detail below in conjunction with Figure 5. As noted above, public key signature methods require the use of a public key 30 and an associated private key which is shown in Figure 2 at 32.

45 The object field 20 (e.g., purchase order data), the type of object field 22, the signing date field 24, the comment field 26, and the signer's certificate field 28 are hashed via a hashing algorithm at 34 to enhance processing efficiency. Additionally, each of the fields 20, 22, 24, 26 and 28 are incorporated in the signature packet 42 to become part of the signature record. A hashing algorithm 44 is also applied to the object 20 to place it in a more compact form prior to incorporation in the packet 42.

50 After application of the hashing algorithm 34 to the fields previously discussed, a presignature hash results therefrom as indicated at 36. The presignature hash 36 is then run through a decrypt (signature) cycle as indicated at 38 using the signer's private key 32 to thereby result in the signer's signature 40. The signer's signature 40 together with items 20 (or the hash of 20), 22, 24, 26 and 28 become the final signature packet 42.

55 When this signature is transmitted with the associated object, it allows the recipient to verify that the object is intact as it was signed. Furthermore, when sufficient certificates are also included, the recipient can validate the true identity of the signer and the authority which has been granted in the signer's chain of certificates.

Turning now to Figure 3, this figure shows how a recipient of the transmitted message, including the signature packet 42 constructed in accordance with Figure 2, verifies the signature. As shown in Figure 3, the recipient utilizes the signature packet 42 and the associated fields 22, 24, 26 and 28 as well as the object 20 and applies the same hashing algorithm 34 as applied to these same fields in Figure 2 to thereby result in a presignature hash 50.

The recipient then utilizes the public encrypting key transmitted with the signer's certificate 28 and performs an encrypt (verification) operation 52 on the signature to be verified 40 (which was transmitted with the signature packet) to thereby generate a presignature hash 54. The recipient, by recomputing the presignature hash in the same way as the signer, then compares this value with the encryption (verification) of the signer's signature.

As indicated at block 56, if these two values at 50 and 54 are not equal, the recipient cannot accept the received signature as being valid. Whether intentional or otherwise, the object and/or the signature must have been changed or tampered with in some way since they were signed. By virtue of this verification step, the recipient determines that the digital signal is consistent with the public key that was named.

In this manner, the object and its signature are processed to insure that the object is identical to the data which existed as it was signed by the owner of the public key. This is the first step of an overall validation process.

Other steps in the validation process insure that the public key belongs to the person named in the associated certificate and that the person has the authority stipulated in the certificate. This verification process applies generally to any object even if that object is another signature or a certificate. To complete the validation process, the recipient analyzes the certificates associated with the signature to determine that the proper authority has been conveyed to each certificate through its signatures and the antecedent certificate(s) of these authorizing signatures.

An object may be accompanied by more than one signature. Such cosignatures fall into the category of either a joint signature or a counter signature. A joint signature is simply another signature of an object by a different party. The signature process is no different than that used to create the initial signature as described in conjunction with Figure 2.

A counter signature is a signature of a signature. Thus, when A signs an object, this signature may itself be thought of as an object. Thus, when C countersigns A's signature, the object C is signing is A's signature itself rather than the original object. The counter signature must therefore occur after the signature being countersigned and reflects approval (or at least recognition) of both the underlying object as well as the fact that A has signed that object. This mechanism allows a chain of authority where each higher level approves any commitment made at a lower level. One of the unique aspects of this system is that the certificate A associates with this signature may in fact require that the use of A's signature be accompanied by particular other joint or counter signatures.

Turning next to the creation of a counter signature which is shown in Figure 4, initially A signs at 63 a primary object 60 in accordance with the procedure outlined in detail in conjunction with Figure 2. The primary object 60 may be a purchase order or some other commitment or it may be a counter signature of some other signature of a primary object.

As explained above in regard to Figure 2, the process of A signing an object may also involve some other party signing A's signature. Thus, A's certificate 62 specifically defines at 65 that, in order for A's signature to be valid (i.e., ratified), a counter signature by C is required, for example, using C's specific certificate Y.

After A signs the object, A's signature packet 66 is then forwarded along with the primary object and all associated signatures and certificates to C and A requests that C add his counter signature 64. Upon receiving the material, C reviews all existing signature certificates and the primary object and if everything meets with his approval he would decide to sign A's signature 68. A's signature inherently reflects the primary object and C's signature inherently reflects A's signature so C will essentially have "signed on the line below A's signature".

Once C decides to approve A's signature at 68, the process of creating a signature as shown in detail in Figure 2, is duplicated except that the object is A's signature. Thus, with A's signature as the object (and the type of object being designated as a signature at 72), the counter signature date 74, C's counter signature comment 76, and C's certificate 70 are applied to a hashing algorithm 80 to thereby result in a presignature hash 82. At the same time, these fields are also inserted into the counter signature packet 88 as discussed above with respect to the signature packet 42 (with a hashing algorithm 69 being applied to the signature object).

Presignature hash 82 and C's secret key 92 are applied in a signature operation 84 to generate a counter signature 86. This counter signature becomes part of the counter signature packet 88 in precisely

the same fashion as described previously in regard to the creation of signature packet 42 in Figure 2.

Because the certificate "Y" which C must use to perform the signature has been explicitly stated (in the certificate which A used to sign), C may also be required to meet his own cosignature obligations so specified by "Y" and forward this entire package including his own newly added signature on to other parties for further cosignatures (either joint or counter signatures). This recursive signature gathering process continues until sufficient signatures are added to fully satisfy all cosignature requirements of at least one party who initially signed the primary object.

Turning next to how one party creates an authorizing certificate for another, it is noted that B creates an authorizing certificate for A by combining a specification of A's identity together with the public encrypting key which A generated for himself. Additionally B specifies the authority capabilities and limitations which B wishes to grant A. By signing the certificate B explicitly assumes responsibility for A's identity and authority.

The present invention permits B to specify other signators who are required to cosign actions taken by A when using the certification. As noted above, B can further define in the certificate for A the degree to which B will recognize subcertifications performed by A.

Additionally, many other limitations and restrictions may be imposed by B. For example, B may impose a money limit which will insure that any recipient of A's certificate will be aware of the limit B is willing to authorize. Since the process of creating a certificate, as will be shown below involves signatures, the use of cosignatures is extended to permit certification authorization. For example, certificates may be designed to allow delegation of subcertification, but only if particular multiple cosigners are involved. This allows checks and balances to be structured into a hierarchy of authority so that electronic digital signatures can be used across organization and institutional boundaries with great confidence --both by the parties receiving the signatures and the parties granting the authority to use the signatures.

The manner in which a party B creates a certificate for party A is shown in Figure 5. As indicated at 100, A creates a public/private key pair in accordance with conventional public key signature systems and supplies the public key to B 102. Once B obtains the public key provided by A for certification, it is important for B to insure that the public key is actually one generated by A and not someone masquerading as A. In this regard, it may be desirable for the public key generated by A to be provided on a face to face basis.

Having selected his own certificate with which to sign A's certificate, B at 106 utilizes the certificate 108 with the associated public key 110 to create a signature of a new certificate 112. As in Figure 2, the signature is created using an object (A's certificate 116) and a certificate (B's certificate 108). B's secret private key is utilized in the decrypt operation to create the signature 112 of the new certificate 116 and the signature packet 114 of B's signature becomes part of A's new certificate packet.

Focussing on the certificate for A which is constructed using information about A specified by B, B builds the certificate by utilizing the public aspect of A's public key as provided by A via line 103. B also sets forth A's full name, A's title and other important statistics such as his address, and telephone number. B may also include a comment to go with the certification which will be available to any person in the future who needs to examine A's certificate.

B additionally will indicate an expiration date of the certificate. This date may reflect the date after which A should not use the certificate. Alternatively, the date may call for any certificate created by A to also expire on this date. B may also indicate in the certificate an account number for A which may represent an internal identification code within B's organization.

Additionally, B may place a monetary limit in the certificate. This monetary authority or credit limit is checked against the limit in B's own certificate to insure that B does not delegate more than he is empowered to delegate. This same relationship is also verified by future recipients as part of their validation process.

As discussed above, B also defines the degree of responsibility to which B is willing is assume for subcertifications done by A. This field must be compatible with the trust level which is allowed B's own certificate. The relationship between the trust level granted to B and that granted by B is another of the relationships validated whenever future recipients validate the hierarchy of certificates which are presented to them.

Finally B inserts cosignature requirements into A's certificate which specify how many and what type of cosignatures are required to accompany A's signature when A uses this new certificate. As indicated above, cosignatures may be in the form of joint signatures and/or counter signatures. The counter signature indicates an approval of the use of the certificate and the approval necessarily follows the associated signature. Joint signatures can be done in any order and do not necessarily reflect approval of the other signatures, but simply approval (or recognition) of a common object.

Cosignature requirements may, for example, be specified in the certificate in a variety of ways. One

technique which may be used is to explicitly define a list of valid joint signers and a list of valid counter signers. Associated with each list is the number specifying the minimum associated signatures which must be present in order for a recipient to recognize the signature as being fully approved. The joint signature list may be a vector of hash values of each of the set of other public keys. Some specified minimum number of these keys must appear in certificates of other signatures applied to any object signed by A when using this new certificate. Otherwise any recipient should not treat A's signature as valid.

The counter signature list is a vector of hash values of other certificates which must be used to sign any signature made under the authority of this certificate. Since this references certificates (rather than public keys), it is possible to reference specific certificates which themselves need further joint or counter signing. By selecting appropriate certificates to appear here, it is possible to create hierarchy of counter signature requirements to whatever a level an organization feels comfortable. A specified number of cosigners is required from each category. This can range from all the candidates to some subset, for example, 0, 1, 2 or 3.

The set of possible co-signers may be indicated explicity in a list as described here, or implicitly by specifying some quality or attribute specification which is designated in each possible co-signer's certificate.

Other fields may be included in the certificate. For example, the current date and time which reflects the moment of the initial creation of the certificate. As indicated in Figure 5, the complete certificate consists of a certificate packet with includes the certificate 116 for A and the signature packet 114 of B's signature to A's certificate.

B's signature and the hierarchy of all certificates and signatures which validate it are kept by A and sent along whenever A uses his certificate. It is contemplated that B or other parties may create several certificates for A. For example, one certificate might allow A to reliably identify himself with no further designated authority. Another certificate might allow authorization to A of certain limited money amounts without requiring any cosignatures. A third might allow authorization for larger amounts but require one or more cosignatures. Still another might allow A to subcertify other persons according to still different money and/or authority limitations and/ or co-signature specifications.

Assuming that B has created a certificate for A as shown in Figure 5, if B requires no cosigners then the certificate is complete. However, the certificate which empowered B to create A's certificate may have required that B have cosigners. There may be one or more joint signature and/or counter signature requirements.

Figure 6 exemplifies the steps taken by party C to jointly certify the certificate of A. The requirement to have a joint signer would be specified in B's own certificate. In this case, a transmitted object (in this case A's new certificate) signed with B's certificate would be rejected by a recipient if C's joint signature is not also present on the object.

As shown in Figure 6, if such a joint signature is required, a copy of B's certificate for A is sent to C who must jointly sign the certificate 120. C then examines A's certificate 122 and verifies that the public key of the certificate actually belongs to A in accordance with process outlined in conjunction with Figure 3.

C then examines the signed attributes and authorizations set forth in the certificate including the assigned monetary level, trust level, etc.. C then, upon concluding that all the fields in B's certificate for A are appropriate, selects his own certificate with which to perform the signature 126. With his own certificate 128, C signs B's certificate of A 132 (130). Once C signs his certificate his signature appears essentially parallel with B's signature and any other cosigners as shown at 134 and 136 of Figure 6. Thus, it is important that C exercise as much caution as B when approving A's certificate. Once A's certificate is created no cosigner may change the certificate for to do so would create essentially a different object to which none of the previous signatures would apply. If C does not approve the certificate he must avoid signing it, and should have a different certificate constructed and re-signed by all necessary parties. After C adds his joint certificate to B's certificate of A, A's certificate packet consists of the certificate for A 132, B's signature packet for A's certificate 134 and finally C's signature packet for A's certificate 136.

In regard to C's signature packet, it is noted that, in order for C to validly sign the certificate, he must select one of his own certificates which grants him sufficient authority to cover what is specified in the new certificate for A. If C has no such certificate, then it is impossible for him to validly sign the certificate since future recipients would reject his certificate as having insufficient authority.

It is noted that C's certificate may also require a counter signature by another party. If so, C forwards the certificate and all associated signatures to the specified party, e.g., D, to counter sign C's signature. When D receives the material he performs the same verification steps as C on the new certificate. If he approves, then D adds his signature to the set. However, D signs C's signature rather then the original certificate object. That is, the object of D's signature is not the object of C's signature (which in this case

was the certificate for A) but rather the object is C's signature itself. This counter signature therefore differs from the joint signature which is simply another signature of the same object.

The application of joint and/or counter signatures can be nested to whatever depth is required, Thus, if D is required to have joint signatures, then this package should be passed to one of D's candidate joint
5 signers for approval of C's signature. This would be a joint counter signature. Similarly, in organizational hierarchies it is possible that D might require counter signatures in which case someone else will need to sign D's signature.

As explained above, the recipient of a primary object (such as a purchase order) and its associated signatures, processes the received materials to insure that the object is identical to the material which
10 existed as it was signed by the owner of the public key. The process for verifying the signature and for verifying that the object had not been tampered with has been explained above in regard to Figure 3.

Additionally, the recipient needs to verify that the identity of the signer is correct and further that the signer has the proper authority within his organization to make the commitments implied by the received object. The sender of the object (e.g., the purchase order) has the responsibility of sending all generations
15 of antecedent certificates and signatures (up to and including the meta-certificate) which are needed for a recipient to perform validation operations.

In validating the object and its signatures, the recipient may, for example proceed as follows. First the recipient insures that the primary object 150 has at least one signature. In the example shown in Figure 7, the primary object 150 has four associated joint signatures 152, 168, 180 and 200, each of which has
20 associated certificates 154, 170, 182 and 202 respectively.

Certificate 154 was made requiring joint signatures by the owners of certificates 170, 182 and 202, and counter-signatures by the owners of certificates 162 and 166 using these specific certificates. The certificate 154 itself was authorized by the owner of certificate 158 as evidenced by signature 156.

In this example, the owner of 154 has obtained the necessary counter signatures 160 and 164 by the
25 holders of certificates 162 and 166, as well as the necessary joint-signatures 168, 180 and 200.

To provide validation for his signature 168, the owner of certificate 170 must include the authorization for his certificate. His certificate was signed by the holder of certificate 174 (as evidenced by 172), however 174's certificate specified that a joint signature by the owner of 178 was required in order to fully ratify 174's signature 172. Thus signature 176 which was made sometime in the past, fulfilled all of 174's joint
30 signature requirements and thereby validated (ratified) the use of 170.

Looking at joint signature 180, by the owner of 182, we learn that 182 requires counter signatures by the holder of 186 using the specific certificate 186. The holder of 182, did in fact get the counter-signature 184 by the holder of 186. However, certificate 186 requires that any signature by 186 itself be countersigned by the holders of certificates 190 and 194 (using these respective certificates). These two holders have
35 in fact countersigned 184 as evidenced by 188 and 192. At one further level we learn that certificate 194 requires any signature by 194 be counter signed by the holder of certificate 198, which signature 196 has been obtained. Certificate 202 requires no co-signature.

All certificates must be accompanied by signatures which are themselves authorized by antecedent certificates. Ultimately all the authority can be traced to a set of certificates which have been signed by the
40 holder of the meta-certificate (or possibly a small set of meta-certificates). Each meta-certificate is well known and distributed to all parties "throughout the world".

The recipient examines every signature supplied and verifies that each accurately signs its purported object (whether the object is a primary object, a certificate, or another signature) using the procedure detailed in Figure 3. The recipient insures that each signature includes a corresponding validated certificate.
45 If a certificate requires joint signatures, then the recipient insures that the required number of these necessary signatures (to the same object) are present. If the certificate requires counter signatures, then the recipient insures that the required number from the designated subset are present (the counter signatures have signatures as their object).

All certificates are then examined. A check is made for the special meta-certificate which has no
50 signature but which is universally known and trusted and a copy of which is already stored in the recipient's computer. If a certificate is received which claims to be the meta-certificate but which is not equal to that already known to and accepted by the recipient, then a rejection is issued. If the meta-certificate is properly recognized, then the validation process continues.

Additionally, a check is made to insure that any other certificate besides the meta-certificate has at least
55 one signature. As noted above, a check is made to insure that all necessary cosignatures for all presented objects are present. Additionally, a check is made to determine that antecedent certificates grant sufficient authority to the subcertificate signers to permit them to validly sign the certificate.

In this regard, the trust value in the certificate must be consistent with the antecedent i.e., the certificate of its signers). By way of example only, the following trust field combinations are valid (using the example specified earlier).

Antecedent Trust Value	Trust Value and Immediate Certificate
0	1
0	2
0	3
1	2
1	3
2	2
2	3

Additionally, any monetary limitations set forth in the certificate must be observed. The money limit allowed by a certificate must not exceed its antecedent. Additionally a check should be made to insure that the antecedent's expiration date is compatible with the antecedent's expiration date. By way of example only, a check may be made to insure that the expiration date in every certificate exceeds the date of each signature which relies on it. In some cases, it may be desirable to reject any material which is controlled by an obsolete certificate.

In order to detect "closed" authority loops (by which a series of certificates may be structured in a loop with the last member of the loop granting authority to the first), it is necessary to insure that all authority ultimately flows from recognized meta-certificates. In this manner, a chain of false or artificial certificates which mutually certify each other will not be inadvertently allowed to incorrectly pass the validation process.

One way to accomplish this is to check off certificates in a series of iterations, starting at the top with the meta-certificate. At each iteration, certificates are scanned and in the process certificates having at least one checked off antecedent would in turn be checked off. The iteration stops when no new certificates have been checked off. If any certificates have not been checked off, then these are "orphans" which should never have been supplied. Such a transmitted package would be rejected.

Once the signatures and certificates are validated (based on the ultimate authority of the meta-certificate(s)), the final step is to insure that the commitment inherent in the primary object is within the authority granted to its immediate (joint) signers. This is done by considering the value imputed to the primary object with the certificates of its signers.

Although the use of a meta-certifier insures that all authority ultimately flows from a trusted source and provides protection, the present invention is not limited to a certification methodology which necessarily includes a single meta-certifier. On the other hand, it is contemplated by the present invention to allow for the use of multiple meta-certifiers. These should be certificates governed by entirely independent sources possibly reflecting the apex of entirely different authorizing hierarchies (e.g., the governmental sector versus the private sector).

Another use of multiple meta-certifiers could be to avoid concentrating full meta-certification responsibility with one group. For example, it might be uncomfortable to know that there is a single entity which could in theory create forgeries on behalf of anyone else by creating false certificates. This concern may be alleviated if the meta-certification authority were distributed among different trusted meta-certifiers. Each meta-certifier would operate completely independently but each certificate would specifically require the others as joint signers. This would essentially eliminate the possibility that isolated corruption within a single organization would compromise the system. For example, any organization that wished to be certified would need to have their own high level master certificate corroborated by each separate entity. Large organizations may likewise wish to structure their own master certificates to be constructed so as to require joint signatures in order to provide multiple safeguards against the danger of isolated corruption within the organization.

While the invention has been described in connection with what is presently considered to be the most practical and preferred embodiment, it is to be understood that the invention is not to be limited to the disclosed embodiment, but on the contrary, is intended to cover various modifications and equivalent arrangements included within the spirit and scope of the appended claims.

Claims

1. In a communications system having a plurality of terminal devices (Terminals A to N) coupled to an insecure communications channel (12) over which users of said terminal devices may exchange private messages, each of said user's having a public key (30) and an associated private key (32), an improved method of digitally signing and certifying a message to be transmitted characterized by the steps of:
formulating at least a portion of a digital message (20);
digitally signing said message (40); and
including within said message an authorizing certificate (28, 116) which specifies the authority which has been granted to the signer of said message.

2. A method according to claim 1, further including the step of providing at least one field in said message identifying the nature of the digital data being transmitted (22).

3. A method according to claim 1, wherein the formulating step includes the step of providing a field allowing the user to insert a predetermined comment (26) regarding the data being transmitted.

4. A method according to claim 1, further including the step of applying a hashing function (34) to at least a portion of the message to be transmitted to form a presignature hash (36); and wherein said digitally signing step includes the step of decrypting said presignature hash with said private decrypting key (32) to form said digital signature.

5. A method according to claim 4, further including the step of forming a digital signature packet (42) comprising the digital signature and a representation of said at least a portion of the message to be transmitted.

6. A method according to claim 1, wherein said authorizing certificate (116) defines the cosignature requirements which must accompany the signer's signature.

7. A method according to claim 6, wherein a digital signature by a third party indicating approval of the user's signature is required (116) thereby defining a counter signature requirement.

8. A method according to claim 7, wherein the third party countersigns (86) by digitally signing the sender's digital signature.

9. A method according to claim 6, wherein the step of defining cosignature requirements includes the step of specifying at least one other digital signature which is required to appear in the digital message thereby defining a joint signature requirement (116).

10. A method according to claim 1, wherein said authorizing certificate defines limitations as to the authority granted by the certificate (116).

11. A method according to claim 10, further including the step of setting a monetary limit for the sender.

12. A method according to claim 1, wherein said authorizing certificate includes at least one field indicative of the degree of responsibility delegated to the sender.

13. A method according to claim 1, wherein said authorizing certificate defines a hierarchy of certificates within the transmitted message such that a recipient of the message can verify the authority of the signer based upon an analysis of the signed message.

COMMUNICATIONS CHANNEL 12

MODEM 6

MODEM 8 ... MODEM 10

TERMINAL A

KEYBOARD/ CRT 4

PROCESSOR W/ MAIN MEMORY 2

TERMINAL B ...

TERMINAL N

FIG.1

FIG.2 CREATE SIGNATURE

OBJECT 20

TYPE OF OBJECT 22

SIGNING DATE 24

COMMENT 26

SIGNER'S CERTIFICATE 28

PUBLIC KEY 30

PRIVATE KEY 32

HASH 34

PRE-SIGNATURE HASH 36

"DECRYPT" 38

HASH 14

SIGNATURE 40

SIGNATURE PACKET 42

FIG.3   VERIFY SIGNATURE

FIG.4

"C" CREATES COUNTER-SIGNATURE FOR A'S SIGNATURE

60 PRIMARY OBJECT

62 "A'S" CERTIFICATE

65 SPECIFIES REQUIRED COUNTER SIGNATURE BY "C" USING CERTIFICATE "Y"

70 C'S CERTIFICATE Y

90 PUBLIC KEY

63 "A" SIGNS OBJECT

66 A'S SIGNATURE PACKET

92 C'S (SECRET) PRIVATE KEY

64 COPIES SENT TO "C" FOR COUNTER SIG.

68 ."EXAMINES PRIMARY OBJ. & DECIDES TO APPROVE 'S SIGNATURE

74 COUNTER SIGNATURE DATE

72 TYPE OF OBJECT "SIGNATURE"

76 C'S COUNTER SIGNATURE COMMENT

80 HASH

82 PRESIGNATURE HASH

84 "DECRYPT"

69 HASH

86 (COUNTER) SIGNATURE

88 (COUNTER SIGNATURE PACKET

FIG.5   "B" CREATES CERTIFICATE
FOR "A"

"A" CREATES
PUBLIC/PRIVATE
PAIR —100

"A" SUPPLIES
PUBLIC ASPECT
TO "B" —102   103

"B" SPECIFIES
INFORMATION
ABOUT "A" —104

"B" SELECTS HIS
OWN CERTIFICATE
WITH WHICH
TO SIGN A'S
CERTIFICATE —106

B'S CERTIFICATE —108

B'S PUBLIC
KEY

—110

112

B CREATES
SIGNATURE
OF NEW
CERTIFICATE

CERTIFICATE FOR "A"
—116

A'S PUBLIC
KEY

A'S NAME
TITLE
ADDRESS
TELEPHONE #
COMMENT BY "B"
EXPIRATION DATE
ACCOUNT #
MONETARY LIMIT

TRUST LEVEL

CO-SIGNATURE
REQUIREMENTS

→MINIMUM # &
LIST OF JOINT-
SIGNER'S PUBLIC
KEY HAS A'S
REQUIREMENTS.
→MINIMUM # &
LIST OF COUNTER-
SIGNER'S CERTIFI-
CATE. HAS A'S
REQUIREMENTS.

CERTIFICATE
PACKET
(CERTIFICATE
WITH
SIGNATURE(S))

114 —

SIGNATURE PACKET
FOR B'S SIGNATURE
TO A'S NEW CERT.

FIG.6 "C" ADDS JOINT SIGNATURE TO "B"'s CERTIFICATE OF "A"

FIG.7 VALIDATION STRUCTURE (EXAMPLE)

COMMUNICATIONS CHANNEL 12

MODEM 6   MODEM 8 ... MODEM 10

TERMINAL A
KEYBOARD/ CRT 4
PROCESSOR W/ MAIN MEMORY 2

TERMINAL B

TERMINAL N

FIG.I

FIG.2   CREATE SIGNATURE

OBJECT 20

TYPE OF OBJECT 22   SIGNING DATE 24   COMMENT 26

SIGNER'S CERTIFICATE 28
PUBLIC KEY 30

PRIVATE KEY 32

HASH 34

PRE-SIGNATURE HASH 36

HASH 44

"DECRYPT" 38

SIGNATURE 40

SIGNATURE PACKET 42

FIG.3 VERIFY SIGNATURE
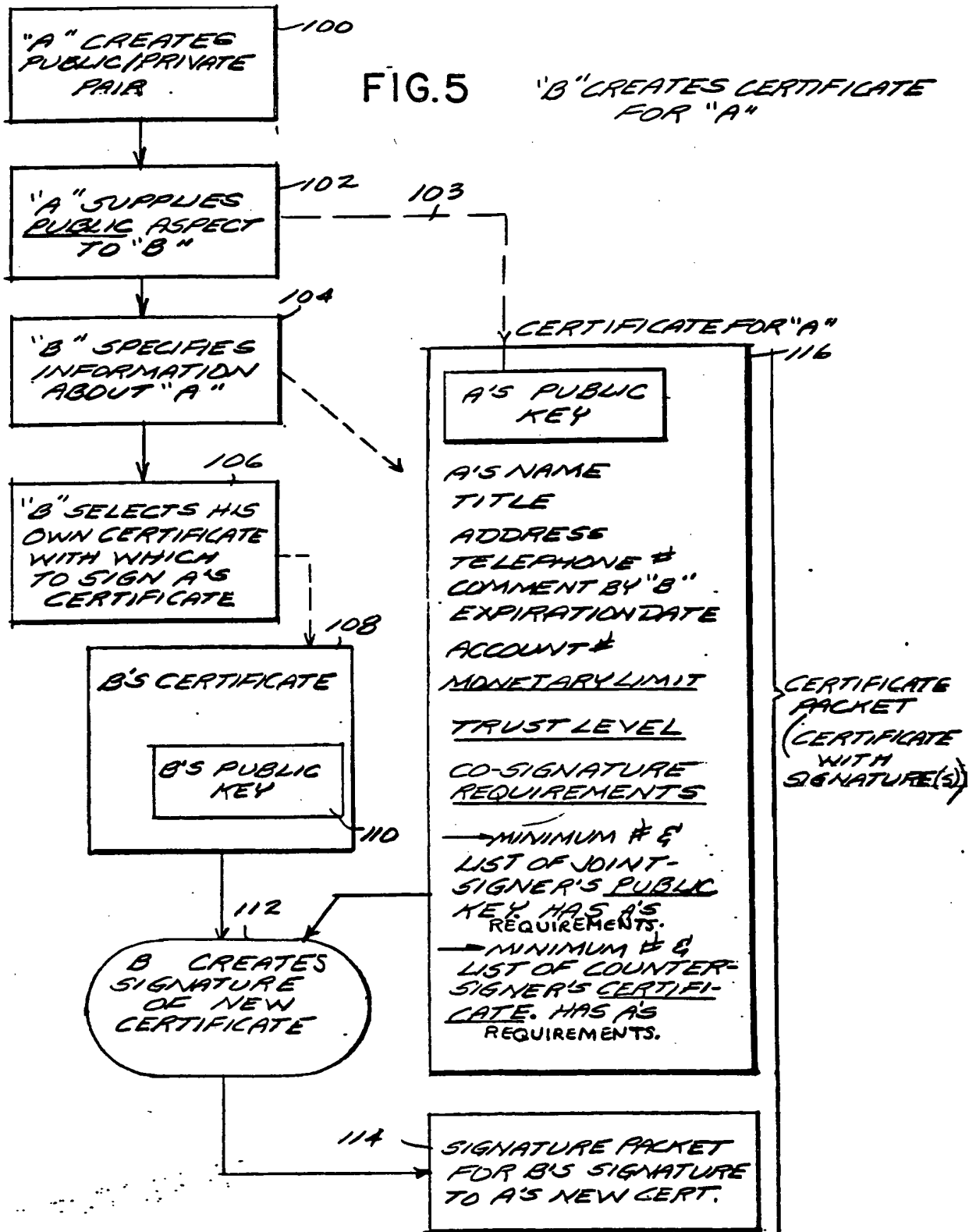
FIG.4 "C" CREATES COUNTER-SIGNATURE FOR A'S SIGNATURE

FIG.5   "B" CREATES CERTIFICATE FOR "A"

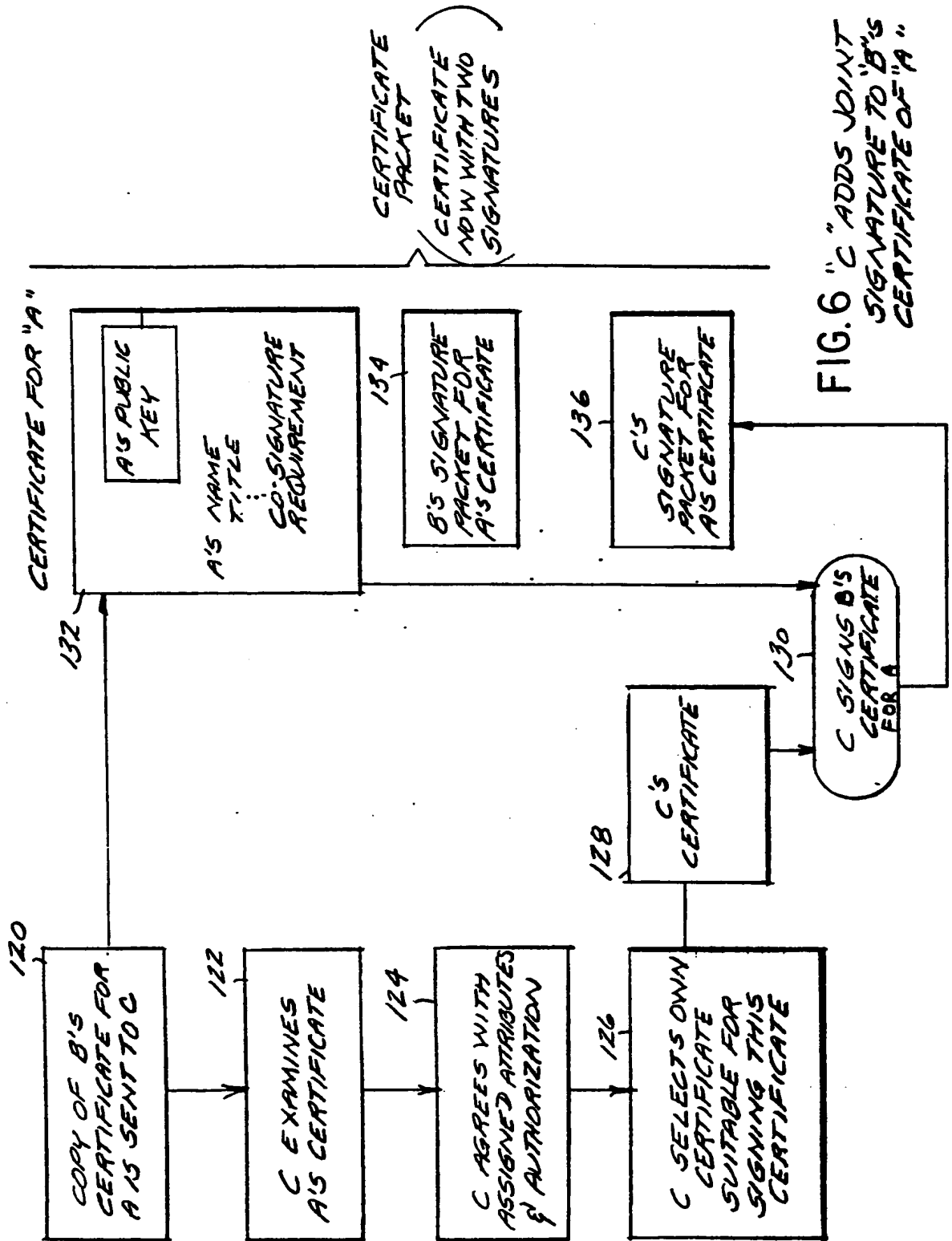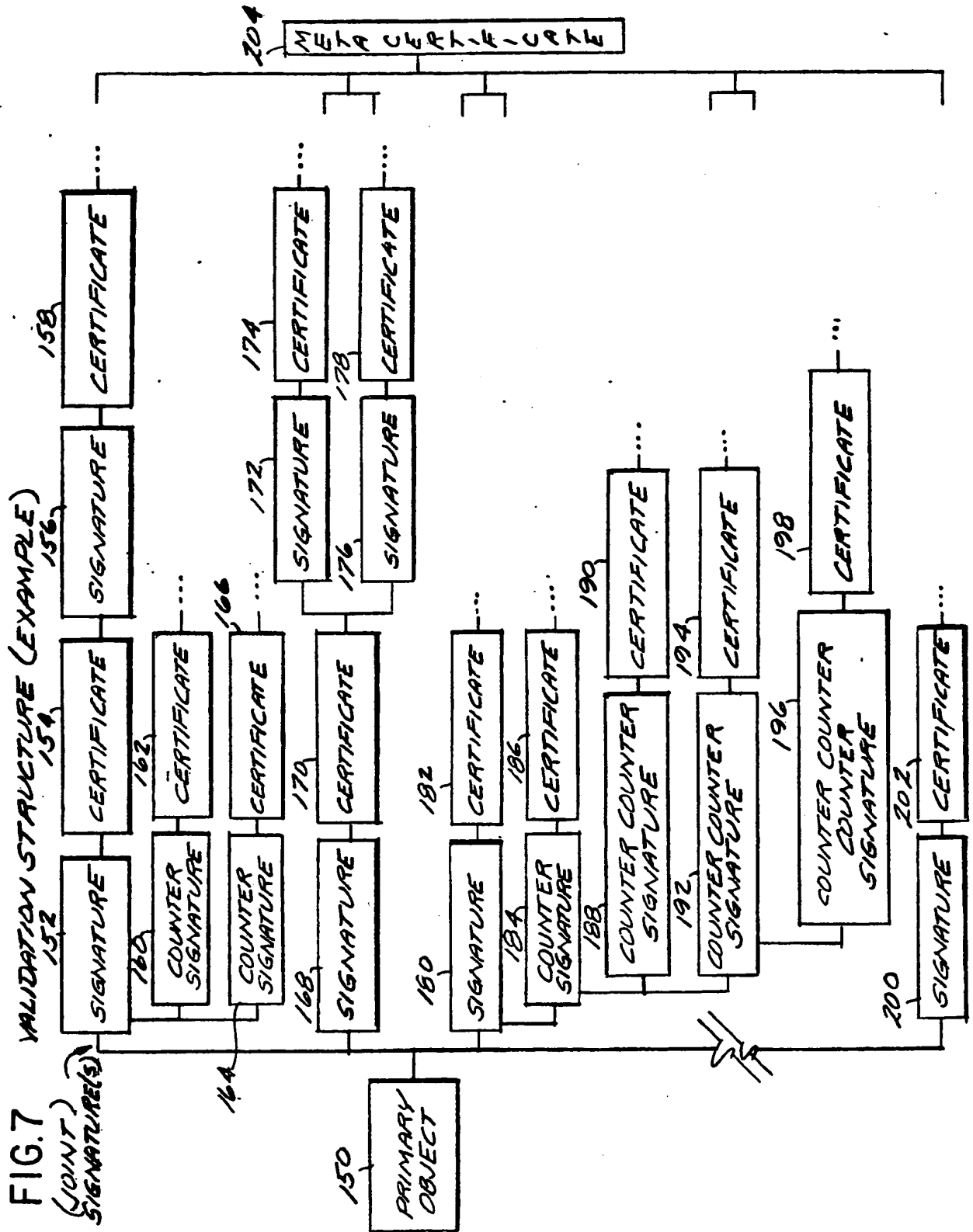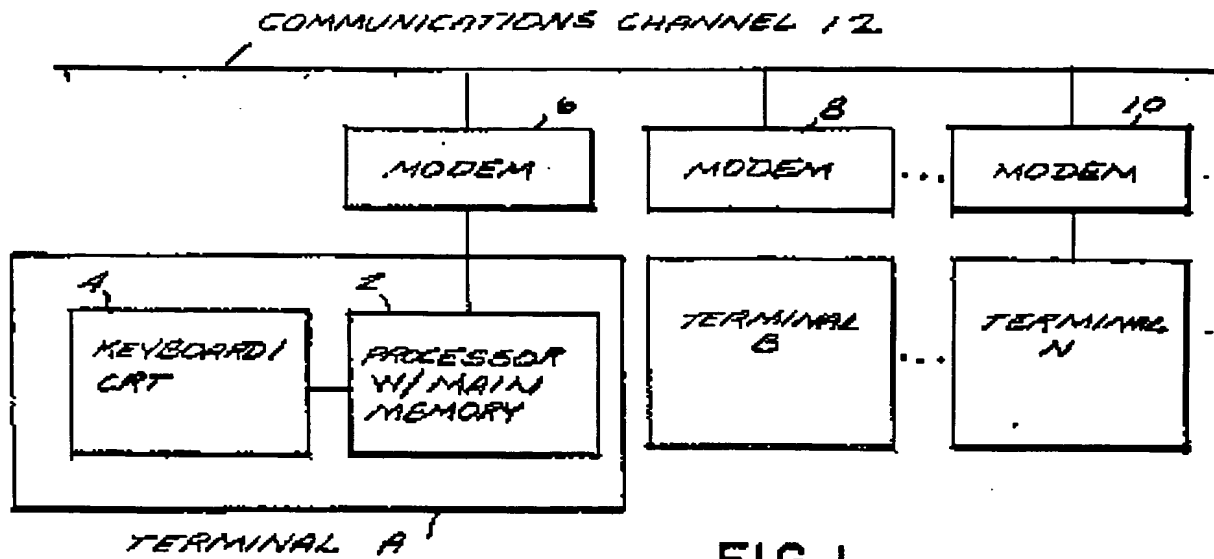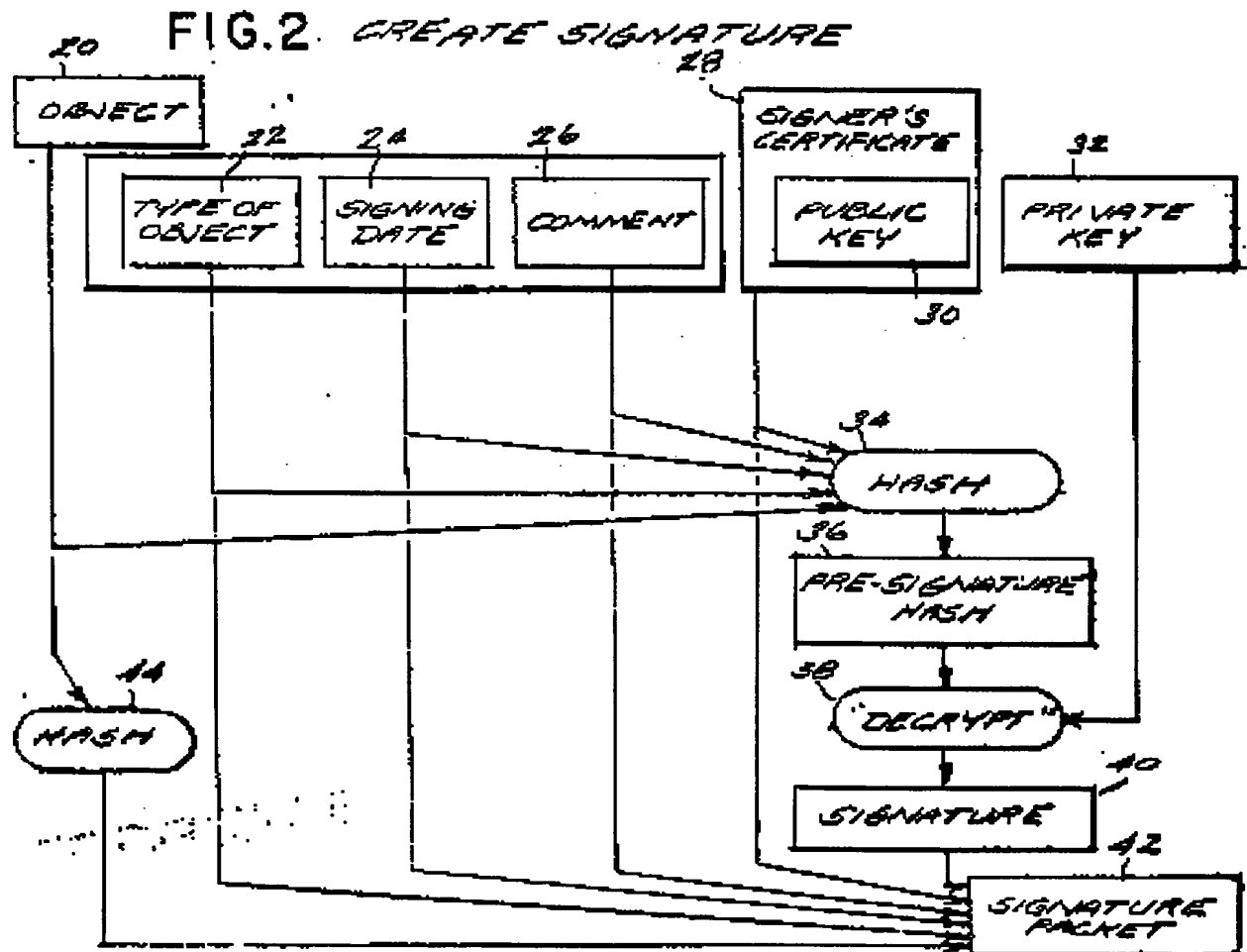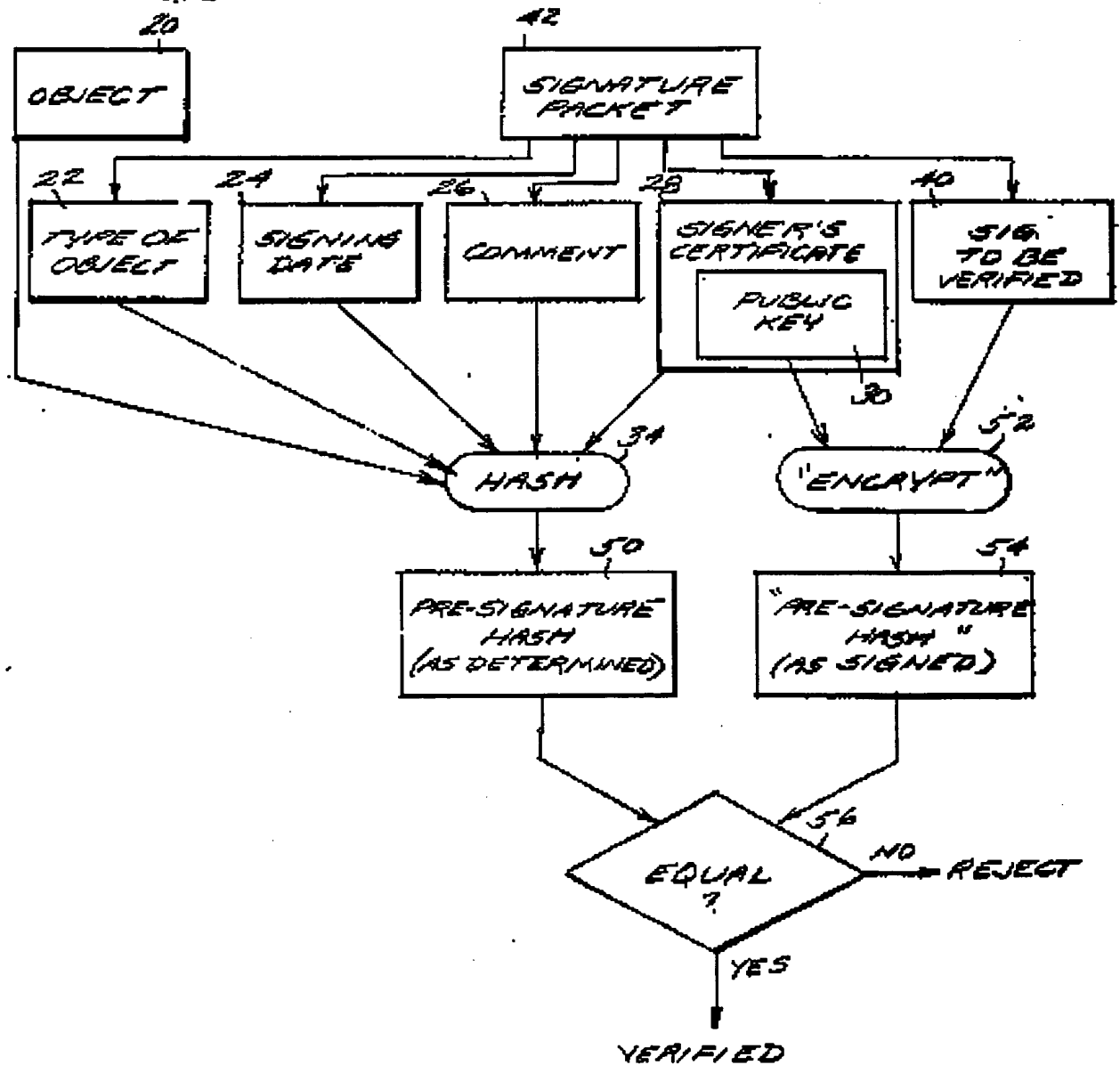"A" CREATES PUBLIC/PRIVATE PAIR — 100

"A" SUPPLIES PUBLIC ASPECT TO "B" — 102   103

"B" SPECIFIES INFORMATION ABOUT "A" — 104

"B" SELECTS HIS OWN CERTIFICATE WITH WHICH TO SIGN A'S CERTIFICATE — 106

B'S CERTIFICATE — 108

B'S PUBLIC KEY

110

B CREATES SIGNATURE OF NEW CERTIFICATE — 112

CERTIFICATE FOR "A"

A'S PUBLIC KEY — 116

A'S NAME

TITLE

ADDRESS

TELEPHONE #

COMMENT BY "B"

EXPIRATION DATE

ACCOUNT #

MONETARY LIMIT

TRUST LEVEL

CO-SIGNATURE REQUIREMENTS

→ MINIMUM # & LIST OF JOINT-SIGNER'S PUBLIC KEY. HAS A'S REQUIREMENTS.

→ MINIMUM # & LIST OF COUNTER-SIGNER'S CERTIFI-CATE. HAS A'S REQUIREMENTS.

CERTIFICATE PACKET (CERTIFICATE WITH SIGNATURE(S))

SIGNATURE PACKET FOR B'S SIGNATURE TO A'S NEW CERT. — 114

CERTIFICATE PACKET

CERTIFICATE
NOW WITH TWO
SIGNATURES

CERTIFICATE FOR "A"

A'S PUBLIC
KEY

A'S NAME
TITLE
...
CO-SIGNATURE
REQUIREMENT

132

B'S SIGNATURE
PACKET FOR
A'S CERTIFICATE

134

C'S
SIGNATURE
PACKET FOR
A'S CERTIFICATE

136

C SIGNS B'S
CERTIFICATE
FOR A

130

C'S
CERTIFICATE

128

COPY OF B'S
CERTIFICATE FOR
A AS SENT TO C

120

C EXAMINES
A'S CERTIFICATE

122

C AGREES WITH
ASSIGNED ATTRIBUTE(S)
& AUTHORIZATION
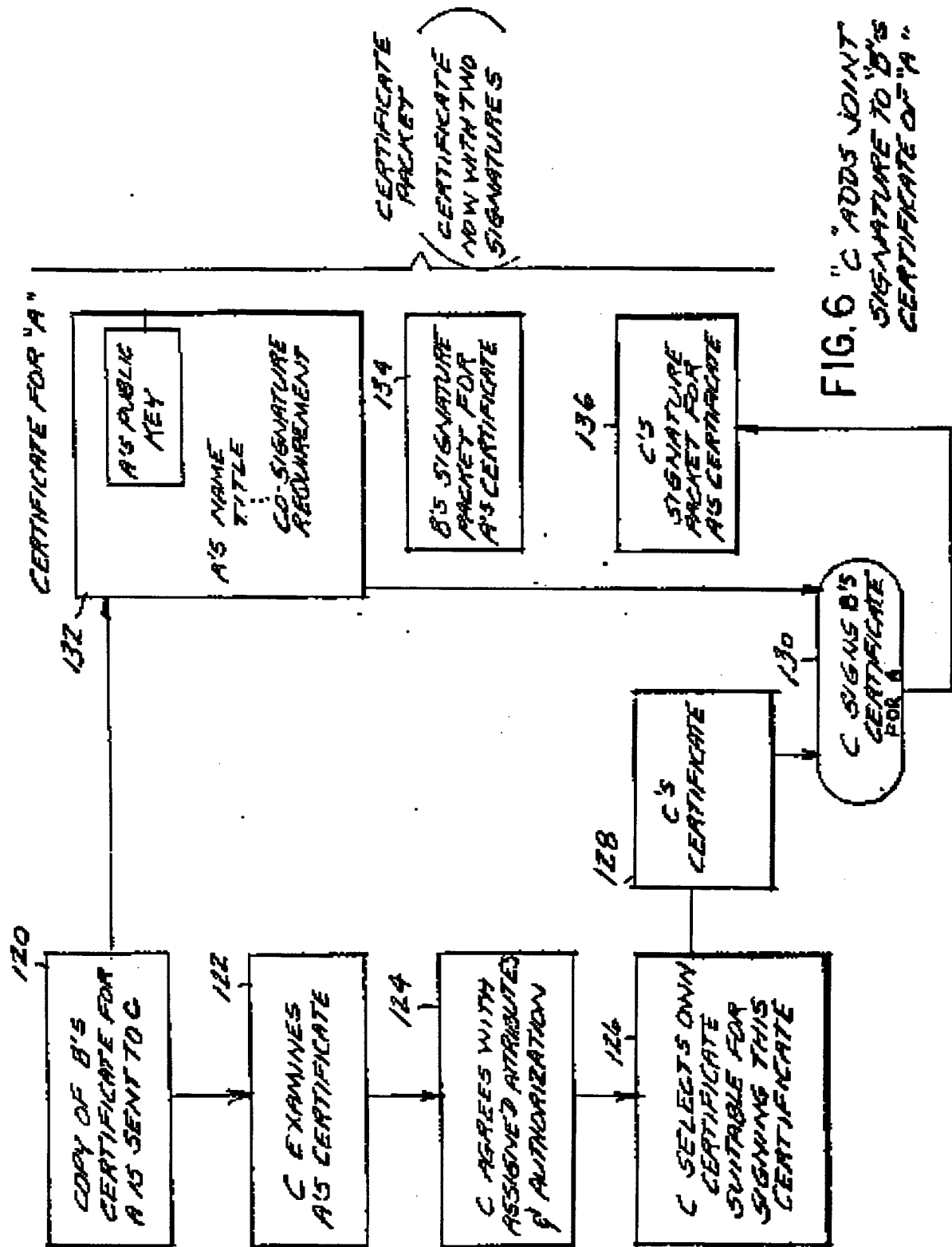
124

C SELECTS OWN
CERTIFICATE
SUITABLE FOR
SIGNING THIS
CERTIFICATE

126

FIG.6 "C" ADDS JOINT
SIGNATURE TO "B'S
CERTIFICATE OF "A"

FIG. 7

VALIDATION STRUCTURE (EXAMPLE)

(JOINT) SIGNATURE(S)